Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/002104

International filing date: 04 February 2005 (04.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-029928
Filing date: 05 February 2004 (05.02.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日本国特許庁
JAPAN PATENT OFFICE

04. 2. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　２月　５日

出願番号
Application Number: 特願２００４－０２９９２８

[ST. 10/C]: ［ＪＰ２００４－０２９９２８］

出願人
Applicant(s): トレンドマイクロ株式会社

２００５年　３月１０日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２０４２４

【書類名】　特許願
【整理番号】　84026
【提出日】　平成16年 2月 5日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 9/00
H04B 17/00

【発明者】
【住所又は居所】　東京都渋谷区代々木２－１－１　トレンドマイクロ株式会社内
【氏名】　近藤　賢志
【発明者】
【住所又は居所】　東京都渋谷区代々木２－１－１　トレンドマイクロ株式会社内
【氏名】　矢田部　茂
【特許出願人】
【識別番号】　397011166
【氏名又は名称】　トレンドマイクロ株式会社
【代理人】
【識別番号】　100098084
【弁理士】
【氏名又は名称】　川▲崎▼　研二
【選任した代理人】
【識別番号】　100111763
【弁理士】
【氏名又は名称】　松本　隆
【手数料の表示】
【予納台帳番号】　038265
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、
前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、
前記判定手段による判定結果を出力する出力手段と
を備えることを特徴とする受信装置。
【請求項２】
受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、
前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、
前記判定手段により実行が許可された場合に前記プログラムを実行する実行手段と
を備えることを特徴とする受信装置。
【請求項３】
受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、
前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、
前記判定手段により実行が許可されなかった場合に、使用可能な機能を制限して前記プログラムを実行するか否かを問い合わせるメッセージを出力する出力手段と、
操作手段と、
前記出力手段によるメッセージの出力に応じて前記操作手段から前記プログラムを実行する旨が指示された場合に、前記プログラムを実行する実行手段と、
前記実行手段により実行されたプログラムにおいて使用可能な機能を、前記登録手段に登録された情報に従って制限する制限手段と
を備えることを特徴とする受信装置。
【請求項４】
前記判定手段は、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されていない場合に、前記プログラムの実行を許可する
ことを特徴とする請求項２または３に記載の受信装置。
【請求項５】
前記登録手段には、受信したプログラムにおいて使用することが許可された関数を示す情報、または前記プログラムにおいて使用することが禁止された関数を示す情報が登録され、
前記機能情報は、前記受信手段により受信されたプログラムに含まれている関数を示す情報である
ことを特徴とする請求項１～３のいずれかに記載の受信装置。
【請求項６】
前記登録手段には、受信したプログラムに従ってアクセスすることが許可されたリソースを示す情報、または前記プログラムに従ってアクセスすることが禁止されたリソースを

示す情報が登録され、
　前記機能情報は、前記受信手段により受信されたプログラムに従ってアクセスされるリソースを示す情報である
　ことを特徴とする請求項１～３のいずれかに記載の受信装置。
【請求項７】
　受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
　プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第１の受信手段と、
　前記第１の受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記プログラムの受信可否を判定する判定手段と、
　前記判定手段により受信が許可された場合に前記プログラムを受信する第２の受信手段と、
　前記第２の受信手段により受信されたプログラムを実行する実行手段と
　を備えることを特徴とする受信装置。
【請求項８】
　ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
　プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、
　前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの中継可否を判定する判定手段と、
　前記判定手段により中継が許可された場合に、前記受信手段により受信された宛先情報によって示される送信先へ前記プログラムを送信する送信手段と
　を備えることを特徴とする中継装置。
【請求項９】
　前記判定手段は、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されていない場合に、前記プログラムの中継を許可する
　ことを特徴とする請求項８に記載の中継装置。
【請求項１０】
　ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、
　プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、
　前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、
　前記判定手段による判定結果と前記プログラムを、前記受信手段により受信された宛先情報によって示される送信先へ送信する送信手段と
　を備えることを特徴とする中継装置。
【請求項１１】
　前記登録手段には、ネットワークを介して提供されるプログラムにおいて使用することが許可された関数を示す情報、または前記プログラムにおいて使用することが禁止された関数を示す情報が登録され、
　前記機能情報は、前記受信手段により受信されたプログラムに含まれている関数を示す情報である
　ことを特徴とする請求項８または１０に記載の中継装置。

【請求項１２】
前記登録手段には、ネットワークを介して提供されるプログラムに従ってアクセスすることが許可されたリソースを示す情報、または前記プログラムに従ってアクセスすることが禁止されたリソースを示す情報が登録され、
前記機能情報は、前記受信手段により受信されたプログラムに従ってアクセスされるリソースを示す情報である
ことを特徴とする請求項８または１０に記載の中継装置。
【請求項１３】
コンピュータに、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する第１のステップと、
予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第１のステップにて受信された機能情報とを比較して、使用することの許可されていない機能が前記第１のステップにて受信されたプログラムにおいて使用されているか否かを判定する第２のステップと、
前記第２のステップにて判定された判定結果を出力する第３のステップと
を実行させるためのプログラム。
【請求項１４】
コンピュータに、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する第１のステップと、
予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第１のステップにて受信された機能情報とを比較して、前記第１のステップにて受信されたプログラムの実行可否を判定する第２のステップと、
前記第２のステップにて実行が許可された場合に前記プログラムを実行する第３のステップと
を実行させるためのプログラム。
【請求項１５】
コンピュータに、
プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第１のステップと、
予めメモリに登録された、受信したプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第１のステップにて受信された機能情報とを比較して、前記機能情報と対応付けられたプログラムの受信可否を判定する第２のステップと、
前記第２のステップにて受信が許可された場合に前記プログラムを受信する第３のステップと、
前記第３のステップにて受信されたプログラムを実行する第４のステップと
を実行させるためのプログラム。
【請求項１６】
コンピュータに、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する第１のステップと、
予めメモリに登録された、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第１のステップにて受信された機能情報とを比較して、前記第１のステップにて受信されたプログラムの中継可否を判定する第２のステップと、
前記第２のステップにて中継が許可された場合に、前記第１のステップにて受信された

宛先情報によって示される送信先へ前記プログラムを送信する第３のステップと
を実行させるためのプログラム。
【請求項１７】
コンピュータに、
プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する第１のステップと、
予めメモリに登録された、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報または前記プログラムにおいて使用することが禁止された機能を示す情報と、前記第１のステップにて受信された機能情報とを比較して、使用することの許可されていない機能が前記第１のステップにて受信されたプログラムにおいて使用されているか否かを判定する第２のステップと、
前記第２のステップにて判定された判定結果と前記プログラムを、前記第１のステップにて受信された宛先情報によって示される送信先へ送信する第３のステップと
を実行させるためのプログラム。
【請求項１８】
請求項１３～１７のいずれかに記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【書類名】明細書
【発明の名称】情報機器上および伝送経路上でのプログラム分析によるセキュリティの確保
【技術分野】
【０００１】
本発明は、情報機器のセキュリティを確保するための技術に関する。
【背景技術】
【０００２】
インターネット等のオープンネットワークでは、様々な人々が自由に情報の公開やプログラムの提供を行うことができる。このため、通信端末に記憶されている個人情報を読み出して通信端末の外部へ密かに送信してしまうプログラム等、通信端末において実行させると、セキュリティ上、問題のあるプログラムがオープンネットワークを介して通信端末に提供されてしまう場合がある。このようなプログラムによって引き起こされる問題から通信端末を保護するため、例えば、特許文献１に記載されたプログラム実行装置では、信頼できるプログラム発信元を示す識別情報（例えば、ＩＰアドレスやＵＲＬ）をメモリに登録しておき、ネットワークを介して受信したプログラムについては、このプログラムの発信元を示す識別情報がメモリに登録されている場合にのみ、プログラムの実行を許可するようにしている。
【特許文献１】特開２００１－１１７７６９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
ところで、特許文献１に記載された技術では、信頼できる全てのプログラム発信元の識別情報をメモリに登録しておかなければならない。したがって、信頼できるプログラム発信元の追加や削除に応じて、メモリに登録されている識別情報を頻繁に更新しなければならず煩雑である。また、インターネットのような大規模なネットワークでは、信頼できるプログラム発信元が極めて多数存在するから、これらの識別情報を漏れなく登録しておくことは実質的に困難である。また、仮に、信頼できる全てのプログラム発信元の識別情報をメモリに登録できたとしても、この場合には、識別情報を登録しておくために必要となるメモリ容量が極めて大きなものとなってしまうから、特に、携帯電話機等の小型の通信端末においては、メモリの容量を増やさなければならない等、コストアップを招いてしまう。
【０００４】
一方で、例えば、通信端末において、ネットワークを介して受信したプログラムの内容を解析し、このプログラムを実行した場合にセキュリティ上の問題が起きないか検証しようとすると、通信端末に高い演算能力が備わっていなければならない。加えて、このような検証処理は負荷が大きく時間もかかる。また、ネットワーク上に設けられたサーバ等の中継装置において、通信端末へ転送するプログラムの内容を解析し、このプログラムを通信端末において実行した場合にセキュリティ上の問題が起きないか検証しようとすると、中継装置に高い演算能力が備わっていなければ、通信の遅延を招いたり、通信網のトラフィックに支障をきたしてしまう。
【０００５】
本発明は、以上説明した事情に鑑みてなされたものであり、その目的は、ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定できるようにすることである。
【課題を解決するための手段】
【０００６】
上記課題を解決するために、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能

を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、前記判定手段による判定結果を出力する出力手段とを備える受信装置を提供する。

【０００７】

また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。このプログラムは、コンピュータのメモリに予めインストールされていてもよいし、ネットワークを介した通信や、上記記録媒体を介してコンピュータにインストールされてもよい。

【０００８】

本発明によれば、受信装置は、使用することの許可されていない機能が、受信したプログラムにおいて使用されているか否かを、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定し、判定結果を出力する。

【０００９】

また、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの実行可否を判定する判定手段と、前記判定手段により実行が許可された場合に前記プログラムを実行する実行手段とを備える受信装置を提供する。また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【００１０】

本発明によれば、受信装置は、受信したプログラムの実行可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。

【００１１】

また、本発明は、受信したプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムを受信する前に、受信するプログラムにおいて使用される機能を示す機能情報を受信する第１の受信手段と、前記第１の受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記プログラムの受信可否を判定する判定手段と、前記判定手段により受信が許可された場合に前記プログラムを受信する第２の受信手段と、前記第２の受信手段により受信されたプログラムを実行する実行手段とを備える受信装置を提供する。また、本発明は、上記受信装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。

【００１２】

本発明によれば、受信装置は、プログラムの受信可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。

【００１３】

また、本発明は、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、前記受信手段により受信されたプログラムの中継可否を判定する判定手段と、前記判定手段により中継が許可された場合に、前記受信手段により受信された宛先情報によって示される送信先へ前記プログラムを送信する送信手段とを備える中継装置を提供する。

【００１４】
また、本発明は、上記中継装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。このプログラムは、コンピュータのメモリに予めインストールされていてもよいし、ネットワークを介した通信や、上記記録媒体を介してコンピュータにインストールされてもよい。
【００１５】
本発明によれば、中継装置は、受信したプログラムの中継可否を、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定する。
【００１６】
また、本発明は、ネットワークを介して提供されるプログラムにおいて使用することが許可された機能を示す情報、または前記プログラムにおいて使用することが禁止された機能を示す情報を登録する登録手段と、プログラムと、当該プログラムにおいて使用される機能を示す機能情報と、当該プログラムの送信先を示す宛先情報とを受信する受信手段と、前記受信手段により受信された機能情報と、前記登録手段に登録された情報とを比較して、使用することの許可されていない機能が前記受信手段により受信されたプログラムにおいて使用されているか否かを判定する判定手段と、前記判定手段による判定結果と前記プログラムを、前記受信手段により受信された宛先情報によって示される送信先へ送信する送信手段とを備える中継装置を提供する。また、本発明は、上記中継装置としてコンピュータを機能させるためのプログラムと、このプログラムを記録したコンピュータ読み取り可能な記録媒体を提供する。
【００１７】
本発明によれば、中継装置は、使用することの許可されていない機能が、受信したプログラムにおいて使用されているか否かを、このプログラムの機能情報と、登録手段に登録された情報とを比較して判定し、判定結果をプログラムとともに送信する。
【発明の効果】
【００１８】
本発明によれば、ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定することができる。
【発明を実施するための最良の形態】
【００１９】
以下、図面を参照して本発明の実施形態について説明する。
［Ａ．第１実施形態］
図１は、第１実施形態に係る通信システム１の構成を例示するブロック図である。同図において、コンテンツプロバイダ１０は、携帯電話機５０にコンテンツを提供する事業者である。コンテンツサーバ１０ａは、インターネット３０および移動パケット通信網４０を介して携帯電話機５０とパケット通信を行うことができる。このコンテンツサーバ１０ａには、携帯電話機５０用のプログラムと、このプログラムを検査機関２０において検査した結果得られる検査結果データ２０２とが記憶されている。なお、コンテンツサーバ１０ａに記憶されているプログラムは、プログラムの実行時に使用される画像データや音声データ等を含んだソフトウェアであってもよい。
【００２０】
検査機関２０は、携帯電話機５０に提供されるプログラムをコンテンツプロバイダ１０からの検査依頼に応じて検査する機関であり、プログラム検査装置２０ａには安全性評価表２０１が記憶されている。この安全性評価表２０１には、携帯電話機５０用のプログラムに含まれている、ファンクションコール、システムコール、機能呼び出し等の各種の関数のうち、ネットワークを介して提供されるプログラムに含まれていた場合、このプログラムを実行すると携帯電話機５０においてセキュリティ上の問題が起きる可能性のある関数の一覧が記録されている。加えて、この安全性評価表２０１には、携帯電話機５０がアクセスすることのできる各種のリソースのうち、ネットワークを介して提供されるプログ

ラムに従ってアクセスされると、携帯電話機５０においてセキュリティ上の問題が起きる可能性のあるリソースの一覧が記録されている。

【００２１】

プログラム検査装置２０ａは、安全性評価表２０１を用いて検査対象となるプログラムを解析し、検査対象となるプログラムから安全性評価表２０１に記録されている関数を抽出する。加えて、プログラム検査装置２０ａは、検査対象となるプログラムを実行した場合にアクセスされるリソースのうち、安全性評価表２０１に記録されているリソースを特定する。そして、プログラム検査装置２０ａは、抽出した関数の名称や、特定したリソースを示す情報（例えば、リソースの格納場所を示すＵＲＬやパス、リソースに割り当てられた識別名等）を収めた検査結果データ２０２を生成する。この検査結果データ２０２がコンテンツプロバイダ１０へと返却され、プログラムに付与されてコンテンツサーバ１０ａに記憶される。

【００２２】

なお、プログラム検査装置２０ａは、検査対象となるプログラムに含まれている全ての関数や、検査対象となるプログラムを実行した場合にアクセスされる全てのリソースを検査結果データ２０２に記録する構成であってもよい。

【００２３】

携帯電話機５０は、移動パケット通信網４０に収容される通信端末（受信装置）であって、コンテンツサーバ１０ａからプログラムをダウンロードしてこれを実行することができる。

【００２４】

次に、図２は、検査結果データ２０２のデータ構成を例示する図である。同図に示すように、検査結果データ２０２には、検査されたプログラムのファイル名と、このプログラムのハッシュ値を算出するために用いたハッシュアルゴリズムの名称と、算出されたハッシュ値とが記録されている。加えて、この検査結果データ２０２には、安全性評価表２０１を用いて検査対象となるプログラムを解析した結果得られた、このプログラムに含まれている関数の名称の一覧や、このプログラムを実行した場合にアクセスされるリソースを示す情報の一覧が記録されている。なお、検査結果データ２０２に記録されたハッシュ値は、プログラム検査装置２０ａによる検査後にプログラムがすり替えられたり改竄されていないことを携帯電話機５０において検証するために用いられる。

【００２５】

図３は、携帯電話機５０のハードウェア構成を例示するブロック図である。同図において、ＣＰＵ５０１は、ＲＯＭ５０２や不揮発性メモリ５０７に記憶されている各種のプログラムを実行することにより携帯電話機５０の各部を制御する。ＲＯＭ５０２には、携帯電話機５０を制御するためのプログラム等が記憶されている。ＲＡＭ５０３は、ＣＰＵ５０１のワークエリアとして用いられる。無線通信部５０４は、ＣＰＵ５０１の制御の下、移動パケット通信網４０の基地局（図示を省略）との間で行われる無線通信を制御する。操作入力部５０５は、複数のキーを有しており、これらのキーの操作に応じた操作信号をＣＰＵ５０１に出力する。液晶表示部５０６は、液晶表示パネルと、この液晶表示パネルの表示制御を行う駆動回路とを有している。

【００２６】

不揮発性メモリ５０７には、例えば、携帯電話機５０のオペレーティングシステムやＷＷＷ（World Wide Web）ブラウザ用のソフトウェアが記憶されている。また、この不揮発性メモリ５０７に、コンテンツサーバ１０ａからダウンロードされたプログラムとその検査結果データ２０２が記憶される。また、不揮発性メモリ５０７には、セキュリティ管理テーブル５０７ａが記憶されている。

【００２７】

セキュリティ管理テーブル５０７ａには、図４に示すように、携帯電話機５０用のプログラムに含まれている各種の関数のうち、ネットワークを介して受信したプログラムを実行する場合に使用することが許可された関数の名称や、逆に、ネットワークを介して受信

したプログラムを実行する場合に使用することが禁止された関数の名称が登録されている。加えて、このセキュリティ管理テーブル５０７ａには、携帯電話機５０がアクセスすることのできる各種のリソースのうち、ネットワークを介して受信したプログラムを実行する場合にアクセスすることが許可されたリソースを示す情報や、逆に、ネットワークを介して受信したプログラムを実行する場合にアクセスすることが禁止されたリソースを示す情報が登録されている。また、プログラムの実行可否をユーザに問い合わせる関数やリソースについては、セキュリティ管理テーブル５０７ａにおいて「許否」の項目に“ユーザ確認”が登録されている。

【００２８】

不揮発性メモリ５０７には、携帯電話機５０に対して設定可能な各セキュリティレベル毎に、例えば、“レベル１”用のセキュリティ管理テーブル５０７ａや、“レベル２”用のセキュリティ管理テーブル５０７ａ等、複数のセキュリティ管理テーブル５０７ａが記憶されている。携帯電話機５０において、ネットワークを介して受信したプログラムの実行可否を判定する際には、上述した複数のセキュリティ管理テーブル５０７ａの中から、現時点において携帯電話機５０に設定されているセキュリティレベルに対応するセキュリティ管理テーブル５０７ａが用いられる。また、セキュリティレベルは、携帯電話機５０のユーザによって設定される。

【００２９】

なお、セキュリティ管理テーブル５０７ａに登録する関数や、各関数についての使用の許否は、携帯電話機５０のユーザが任意に変更できる構成であってもよい。これはセキュリティ管理テーブル５０７ａに登録するリソースや、各リソースについてのアクセスの許否についても同様である。

【００３０】

次に、第１実施形態の動作について説明する。

図５は、プログラムとその検査結果データ２０２が携帯電話機５０にダウンロードされるまでの通信システム１各部の動作について例示するシーケンスチャートである。同図に示すように、例えば、コンテンツプロバイダ１０によって作成された携帯電話機５０用のプログラムは、検査依頼要求とともにコンテンツサーバ１０ａからプログラム検査装置２０ａへと送信される（ステップＳ１０１）。

【００３１】

プログラム検査装置２０ａは、プログラムおよび検査依頼要求を受信すると、受信したプログラムを解析する（ステップＳ１０２）。プログラム検査装置２０ａは、受信したプログラムから安全性評価表２０１に記録されている関数を抽出するとともに、受信したプログラムを実行した場合にアクセスされるリソースのうち、安全性評価表２０１に記録されているリソースを特定する。また、プログラム検査装置２０ａは、任意のハッシュアルゴリズムを用いて、受信したプログラムのハッシュ値を算出する。そして、プログラム検査装置２０ａは、抽出した関数の名称や、特定したリソースを示す情報に加え、算出したハッシュ値や、使用したハッシュアルゴリズムの名称、受信したプログラムのファイル名等を収めた検査結果データ２０２を生成する（ステップＳ１０３）。

【００３２】

また、プログラム検査装置２０ａは、生成した検査結果データ２０２に電子署名を施す（ステップＳ１０４）。この電子署名は、プログラム検査装置２０ａによって生成された検査結果データ２０２が、すり替えられたり改竄されていないことを携帯電話機５０において検証するために用いられる。この後、プログラム検査装置２０ａは、電子署名が施された検査結果データ２０２をコンテンツサーバ１０ａへ返信する（ステップＳ１０５）。コンテンツサーバ１０ａは、検査結果データ２０２を受信すると、この検査結果データ２０２を、検査対象となったプログラムに付加してメモリに記憶し（ステップＳ１０６）、プログラムとその検査結果データ２０２を携帯電話機５０からダウンロード可能な状態とする。

【００３３】

一方、携帯電話機５０では、まず、セキュリティレベルを設定する処理が行われる（ステップＳ１０７）。このセキュリティレベルの設定に際しては、例えば、図６に示すような画像が液晶画面に表示され、ユーザは、操作入力部５０５を操作して、携帯電話機５０に設定するセキュリティレベルを“レベル０（なし）”～“レベル５”の中から任意に選択することができる。また、ユーザによって設定されたセキュリティレベルの値は、不揮発性メモリ５０７に記憶される。

【００３４】

この後、コンテンツサーバ１０ａからプログラムをダウンロードする際には、まず、携帯電話機５０においてＷＷＷブラウザが起動され（ステップＳ１０８）、携帯電話機５０とコンテンツサーバ１０ａとの間でパケット通信が開始される。そして、ユーザが操作入力部５０５を操作してダウンロードするプログラムを指定すると、このプログラムのダウンロードを要求する信号が携帯電話機５０からコンテンツサーバ１０ａへと送信される（ステップＳ１０９）。コンテンツサーバ１０ａは、ダウンロードの要求を受けたプログラムと、このプログラムの検査結果データ２０２とをメモリから読み出して携帯電話機５０へ送信し（ステップＳ１１０，Ｓ１１１）、携帯電話機５０は、プログラムと検査結果データ２０２を受信すると、これらを不揮発性メモリ５０７に記憶する（ステップＳ１１２）。

【００３５】

次に、図７は、携帯電話機５０において実行される、ネットワークを介して受信したプログラムの実行可否を判定する処理の動作を例示するフローチャートである。この処理は、携帯電話機５０において、ネットワークを介して受信したプログラムを実行する旨が指示された場合に、ＣＰＵ５０１により実行される。同図に示すように、まず、ＣＰＵ５０１は、実行する旨が指示されたプログラムの検査結果データ２０２を不揮発性メモリ５０７から読み出す（ステップＳ２０１）。

【００３６】

次いで、ＣＰＵ５０１は、読み出した検査結果データ２０２の電子署名を検証し（ステップＳ２０２）、この検査結果データ２０２が検査機関２０によって生成されたものであって、改竄等が行われていない正当な検査結果データ２０２であることを確認する。その結果、正当な検査結果データ２０２でないことが判った場合（ステップＳ２０３：ＮＯ）、ＣＰＵ５０１は、プログラムの実行を中止し（ステップＳ２１０）、検査結果データ２０２に改竄等の不正が見つかったため、プログラムの実行を中止したことを示すメッセージを液晶画面に表示する。

【００３７】

一方、正当な検査結果データ２０２であることが検証された場合（ステップＳ２０３：ＹＥＳ）、ＣＰＵ５０１は、検査結果データ２０２に記録されているハッシュアルゴリズムを用いて、実行する旨が指示されたプログラムのハッシュ値を算出する。次いで、ＣＰＵ５０１は、算出したハッシュ値と、検査結果データ２０２に記録されているハッシュ値とを照合する（ステップＳ２０４）。その結果、ハッシュ値が一致しなかった場合（ステップＳ２０５：ＮＯ）、ＣＰＵ５０１は、プログラムの実行を中止し（ステップＳ２１０）、プログラムに改竄等の不正が見つかったため、プログラムの実行を中止したことを示すメッセージを表示する。

【００３８】

また、ハッシュ値が一致した場合（ステップＳ２０５：ＹＥＳ）、ＣＰＵ５０１は、現時点において携帯電話機５０に設定されているセキュリティレベルの値を特定し、特定したセキュリティレベルの値に対応するセキュリティ管理テーブル５０７ａを不揮発性メモリ５０７から読み出す（ステップＳ２０６）。そして、ＣＰＵ５０１は、読み出したセキュリティ管理テーブル５０７ａと、ステップＳ２０１において取得した検査結果データ２０２とを比較して（ステップＳ２０７）、実行する旨が指示されたプログラムの実行可否を判定する（ステップＳ２０８）。

【００３９】

このステップＳ２０７，Ｓ２０８における処理について具体的に説明すると、まず、ＣＰＵ５０１は、検査結果データ２０２に記録されている各関数、すなわち、実行する旨が指示されたプログラムから抽出された各関数毎に、この関数がセキュリティ管理テーブル５０７ａにおいて使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。同様に、ＣＰＵ５０１は、検査結果データ２０２に記録されている各リソース毎に、このリソースがセキュリティ管理テーブル５０７ａにおいてアクセスを許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。

【００４０】

その結果、ＣＰＵ５０１は、使用が禁止された関数が検査結果データ２０２に１つでも記録されていた場合や、アクセスが禁止されたリソースが検査結果データ２０２に１つでも記録されていた場合に、実行する旨が指示されたプログラムは、ユーザによって設定されたセキュリティポリシー（セキュリティ管理テーブル５０７ａ）に違反するものであると判断し、このプログラムの実行を許可しない（ステップＳ２０８：ＮＯ）。この場合、ＣＰＵ５０１は、プログラムの実行を中止し（ステップＳ２１０）、例えば、図８に示すようなメッセージを液晶画面に表示する。

【００４１】

例えば、検査結果データ２０２が図２に示すものである一方、セキュリティ管理テーブル５０７ａが図４に示すものであった場合、検査結果データ２０２には、セキュリティ管理テーブル５０７ａにおいて使用が禁止された関数“Function１()”や、セキュリティ管理テーブル５０７ａにおいてアクセスが禁止されたリソース“Local/UserData/Address Book”が記録されているから、この検査結果データ２０２が付与されているプログラムは、携帯電話機５０において実行が許可されない。

【００４２】

一方、ＣＰＵ５０１は、検査結果データ２０２に記録されている全ての関数がセキュリティ管理テーブル５０７ａにおいて使用を許可された関数であって、かつ、検査結果データ２０２に記録されている全てのリソースがセキュリティ管理テーブル５０７ａにおいてアクセスを許可されたリソースであった場合に、実行する旨が指示されたプログラムは、ユーザによって設定されたセキュリティポリシーを満たすものであると判断し、このプログラムの実行を許可する（ステップＳ２０８：ＹＥＳ）。この場合、ＣＰＵ５０１は、実行することが許可されたプログラムを不揮発性メモリ５０７から読み出して起動し（ステップＳ２０９）、このプログラムに従った処理を開始する。

【００４３】

なお、図４に示したセキュリティ管理テーブル５０７ａにおけるリソース“http:// www.xxx.co.jp”のように、「許否」の項目に“ユーザ確認”が登録されているリソースが検査結果データ２０２に記録されていた場合、ＣＰＵ５０１は、プログラムの実行可否をユーザに問い合わせるメッセージを生成して液晶画面に表示し、操作入力部５０５からの指示に従ってプログラムの実行可否を決定する。

【００４４】

以上説明したように本実施形態によれば、プログラム検査装置２０ａは、ネットワークを介して携帯電話機５０に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ２０２を生成する。携帯電話機５０は、ネットワークを介して受信したプログラムの実行可否を、このプログラムの検査結果データ２０２と、各関数についての使用許否や各リソースについてのアクセスの許否が登録されたセキュリティ管理テーブル５０７ａとを比較して判定する。したがって、携帯電話機５０は、受信したプログラムを解析せずとも、検査結果データ２０２とセキュリティ管理テーブル５０７ａとを比較するだけで、このプログラムが携帯電話機５０に設定されたセキュリティポリシー（セキュリティ管理テーブル５０７ａ）を満たすプログラムであるか否かを判定することができる。よって、このような判定処理を携帯電話機５０において簡易な構成で短時間

のうちに済ますことができる。

【００４５】

また、受信したプログラムの実行可否を判定するために用いるセキュリティ管理テーブル５０７ａは、セキュリティレベルを変更することによって容易に変更可能である。したがって、例えば、セキュリティポリシーに違反するとして実行が認められなかったプログラムであっても、ユーザ自身がこのプログラムは十分に信頼し得るものであると判断した場合は、一時的にセキュリティレベルを下げて、このプログラムを携帯電話機５０において実行すること等が可能となる。このように本実施形態によれば、受信したプログラムに対する携帯電話機５０のセキュリティを、ユーザの意向に応じて柔軟に設定することができるという効果も奏する。

【００４６】

［Ｂ．第２実施形態］

次に、本発明の第２実施形態について説明する。

なお、本実施形態において、第１実施形態と共通する部分については同一の符号を使用するものとする。また、第１実施形態と共通する部分についてはその説明を省略するものとする。

【００４７】

図９は、コンテンツサーバ１０ａと携帯電話機５０との間で行われるパケット通信を中継する中継装置６０のハードウェア構成を例示するブロック図である。なお、この中継装置６０は、インターネット３０上に設けられていてもよいし、移動パケット通信網４０に設けられていてもよい。同図において、通信インタフェース６０４は、ＣＰＵ６０１の制御の下、コンテンツサーバ１０ａや携帯電話機５０との間で行われるパケット通信を制御する。操作入力部６０５は、キーボードやマウスを備え、これらの操作に応じた操作信号をＣＰＵ６０１に出力する。表示部６０６は、ＬＣＤやＣＲＴディスプレイ等である。

【００４８】

ＨＤ（ハードディスク）６０７には、第１実施形態において説明したセキュリティ管理テーブル５０７ａが記憶されている。本実施形態における中継装置６０は、このセキュリティ管理テーブル５０７ａを用いて、コンテンツサーバ１０ａから携帯電話機５０に宛てて送信されたプログラムの中継可否を判定する。なお、中継装置６０は、コンテンツサーバ１０ａからプログラムとともに、このプログラムの検査結果データ２０２と、このプログラムの送信先を示す宛先情報とを受信するが、検査結果データ２０２は、第１実施形態において説明したプログラム検査装置２０ａによって生成されたものである。また、宛先情報は、例えばＩＰアドレス等の、携帯電話機５０に対して割り当てられた通信アドレスである。

【００４９】

また、本実施形態においては、移動パケット通信網４０の通信事業者や中継装置６０の管理者等によって、中継装置６０に対し、セキュリティレベルが設定される。ＨＤ６０７には、第１実施形態において説明したように、セキュリティレベル毎に異なるセキュリティ管理テーブル５０７ａが記憶されており、中継装置６０に対して設定されたセキュリティレベルによって、プログラムの中継可否を判定する際に用いるセキュリティ管理テーブル５０７ａが決定される。

【００５０】

図１０は、中継装置６０において実行される、プログラムの中継可否を判定する処理の動作を例示するフローチャートである。この処理は、コンテンツサーバ１０ａから携帯電話機５０に宛てて送信されたプログラムとその検査結果データ２０２を中継装置６０が受信した場合に、ＣＰＵ６０１により実行される。同図に示すように、まず、ＣＰＵ６０１は、受信した検査結果データ２０２の電子署名を検証する（ステップＳ３０１）。その結果、ＣＰＵ６０１は、正当な検査結果データ２０２でないことが判った場合（ステップＳ３０２：ＮＯ）、携帯電話機５０に対するプログラムの転送を中止し（ステップＳ３０９）、プログラムに付与されている検査結果データ２０２に改竄等の不正が見つかったため

、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機５０へ送信する。

【００５１】

一方、正当な検査結果データ２０２であることが検証された場合（ステップＳ３０２：ＹＥＳ）、ＣＰＵ６０１は、検査結果データ２０２に記録されているハッシュアルゴリズムを用いて、受信したプログラムのハッシュ値を算出し、検査結果データ２０２に記録されているハッシュ値と照合する（ステップＳ３０３）。その結果、ＣＰＵ６０１は、ハッシュ値が一致しなかった場合（ステップＳ３０４：ＮＯ）、携帯電話機５０に対するプログラムの転送を中止し（ステップＳ３０９）、プログラムに改竄等の不正が見つかったため、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機５０へ送信する。

【００５２】

また、ハッシュ値が一致した場合（ステップＳ３０４：ＹＥＳ）、ＣＰＵ６０１は、現時点において中継装置６０に設定されているセキュリティレベルの値を特定し、特定したセキュリティレベルの値に対応するセキュリティ管理テーブル５０７ａをＨＤ６０７から読み出す（ステップＳ３０５）。そして、ＣＰＵ６０１は、読み出したセキュリティ管理テーブル５０７ａと、受信した検査結果データ２０２とを比較して（ステップＳ３０６）、携帯電話機５０に対するプログラムの中継可否を判定する（ステップＳ３０７）。

【００５３】

このステップＳ３０６，Ｓ３０７における処理について具体的に説明すると、まず、ＣＰＵ６０１は、検査結果データ２０２に記録されている各関数、すなわち、受信したプログラムから抽出された各関数毎に、この関数がセキュリティ管理テーブル５０７ａにおいて使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。同様に、ＣＰＵ６０１は、検査結果データ２０２に記録されている各リソース毎に、このリソースがセキュリティ管理テーブル５０７ａにおいてアクセスを許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。

【００５４】

その結果、ＣＰＵ６０１は、使用が禁止された関数が検査結果データ２０２に１つでも記録されていた場合や、アクセスが禁止されたリソースが検査結果データ２０２に１つでも記録されていた場合に、転送されてきたプログラムは、移動パケット通信網４０の通信事業者等によって設定されたセキュリティポリシー（セキュリティ管理テーブル５０７ａ）に違反するものであると判断し、このプログラムの携帯電話機５０への中継を許可しない（ステップＳ３０７：ＮＯ）。この場合、ＣＰＵ６０１は、プログラムの転送を中止し（ステップＳ３０９）、セキュリティポリシーに違反するプログラムであったため、プログラムのダウンロードを中止したことを示すメッセージを携帯電話機５０へ送信する。

【００５５】

一方、ＣＰＵ６０１は、検査結果データ２０２に記録されている全ての関数がセキュリティ管理テーブル５０７ａにおいて使用を許可された関数であって、かつ、検査結果データ２０２に記録されている全てのリソースがセキュリティ管理テーブル５０７ａにおいてアクセスを許可されたリソースであった場合に、転送されてきたプログラムは、通信事業者等によって設定されたセキュリティポリシーを満たすものであると判断し、このプログラムの携帯電話機５０への中継を許可する（ステップＳ３０７：ＹＥＳ）。この場合、ＣＰＵ６０１は、宛先情報によって示される携帯電話機５０へプログラムを転送する（ステップＳ３０８）。

【００５６】

以上説明したように本実施形態によれば、プログラム検査装置２０ａは、ネットワークを介して携帯電話機５０に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ２０２を生成する。中継装置６０は、携帯電話機５０に対するプログラムの中継可否を、このプログラムの検査結果データ２０２と、各関数につい

ての使用許否や各リソースについてのアクセスの許否が登録されたセキュリティ管理テーブル５０７ａとを比較して判定する。したがって、中継装置６０は、転送するプログラムを解析せずとも、検査結果データ２０２とセキュリティ管理テーブル５０７ａとを比較するだけで、このプログラムが中継装置６０に設定されたセキュリティポリシー（セキュリティ管理テーブル５０７ａ）を満たすプログラムであるか否かを判定することができる。よって、このような判定処理を中継装置６０において簡易な構成で短時間のうちに済ますことができ、通信の遅延を招いたり、通信網のトラフィックに支障をきたすようなことがない。また、セキュリティポリシーに違反するプログラムについては転送を中止するから、携帯電話機５０への提供を未然に防ぐことができる。

【００５７】

なお、セキュリティ管理テーブル５０７ａに登録する関数や、各関数についての使用の許否は、移動パケット通信網４０の通信事業者や中継装置６０の管理者等によって任意に変更可能である。勿論、セキュリティ管理テーブル５０７ａに登録するリソースや、各リソースについてのアクセスの許否についても同様である。

【００５８】

［Ｃ．変形例］

（１）第１実施形態では、検査結果データ２０２がプログラムに付与されて携帯電話機５０へ送信されてくる場合について説明した。しかしながら、図１１に示すように、検査結果登録サーバ７０を設け、この検査結果登録サーバ７０に、検査機関２０において検査された各プログラムの検査結果データ２０２が登録される構成としてもよい。この場合、携帯電話機５０は、コンテンツサーバ１０ｂからプログラムをダウンロードした後に、このプログラムの検査結果データ２０２を検査結果登録サーバ７０から取得する。また、第２実施形態についても同様であって、検査結果登録サーバ７０に各プログラムの検査結果データ２０２が登録され、中継装置６０は、携帯電話機５０へ転送するプログラムをコンテンツサーバ１０ｂから受信すると、このプログラムの検査結果データ２０２を検査結果登録サーバ７０から取得するようにしてもよい。なお、検査結果登録サーバ７０は、移動パケット通信網４０に設けられていてもよいし、検査機関２０内に設けられていてもよい。

【００５９】

（２）第１実施形態において、図７に示したフロチャートのステップＳ２０８にてＮＯと判定された場合以降の処理を、図１２に示すように変形してもよい。

すなわち、ＣＰＵ５０１は、図７のステップＳ２０８にてＮＯと判定された場合に、まず、図１３に示すように、実行する旨が指示されたプログラムがセキュリティポリシーに違反していることと、使用可能な機能を制限した上でこのプログラムを実行するか否かを問い合わせるメッセージを液晶画面に表示する（ステップＳ４０１）。このメッセージの表示に応じてユーザは、使用可能な機能を制限してプログラムを実行することとするのか、それともプログラムの実行を中止するのかを、操作入力部５０５を操作して携帯電話機５０に指示する。なお、上記メッセージは、音声メッセージとして携帯電話機５０から出力されてもよい。

【００６０】

ＣＰＵ５０１は、プログラムの実行を中止する旨が操作入力部５０５から指示された場合（ステップＳ４０２：ＮＯ）、プログラムの実行を中止する（ステップＳ４０３）。一方、ＣＰＵ５０１は、プログラムを実行する旨が操作入力部５０５から指示された場合（ステップＳ４０２：ＹＥＳ）、実行する旨が指示されたプログラムを不揮発性メモリ５０７から読み出して起動する（ステップＳ４０４）。次いで、ＣＰＵ５０１は、プログラムの実行が終了したか否かを判別し（ステップＳ４０５）、プログラムの実行が終了するまでの間、このプログラムにおいて使用可能な機能を、セキュリティ管理テーブル５０７ａに従って制限する（ステップＳ４０６）。なお、使用可能な機能を制限する際に用いるセキュリティ管理テーブル５０７ａは、現時点において携帯電話機５０に設定されているセキュリティレベルに対応するものである。

【００６１】

このステップＳ４０６における処理について具体的に説明すると、まず、ＣＰＵ５０１は、プログラムを順次解釈して実行していく際に、ファンクションコール、システムコール、機能呼び出し等の関数があった場合、この関数がセキュリティ管理テーブル５０７ａにおいて使用を許可された関数であるのか、それとも使用が禁止された関数であるのかを特定する。そして、ＣＰＵ５０１は、使用が許可された関数であった場合に、この関数の使用を許可してプログラムの実行を継続する一方、使用が禁止された関数であった場合は、この関数の使用を許可せず、プログラムの実行を中止する。

【００６２】

また、ＣＰＵ５０１は、プログラムを順次解釈して実行していく過程で発生する、各種リソースへのアクセス要求を監視し、アクセス要求のあったリソースがセキュリティ管理テーブル５０７ａにおいてアクセスが許可されたリソースであるのか、それともアクセスが禁止されたリソースであるのかを特定する。そして、ＣＰＵ５０１は、アクセスが許可されたリソースであった場合に、このリソースに対するアクセスを許可してプログラムの実行を継続する一方、アクセスが禁止されたリソースであった場合は、このリソースに対するアクセスを許可せず、プログラムの実行を中止する。

【００６３】

以上説明した構成とすれば、携帯電話機５０では、セキュリティポリシーに違反するプログラムであっても、使用可能な機能を制限した上でこのプログラムを実行することができる。

【００６４】

（３）セキュリティ管理テーブル５０７ａには、使用が許可された関数と使用が禁止された関数の情報のみが登録されていてもよい。また、逆に、アクセスが許可されたリソースとアクセスが禁止されたリソースの情報のみがセキュリティ管理テーブル５０７ａに登録されていてもよい。さらに、使用が許可された関数の情報のみ、あるいは使用が禁止された関数の情報のみがセキュリティ管理テーブル５０７ａに登録されていてもよいし、アクセスが許可されたリソースの情報のみ、あるいはアクセスが禁止されたリソースの情報のみがセキュリティ管理テーブル５０７ａに登録されていてもよい。

【００６５】

（４）第２実施形態において、中継装置６０のＨＤ６０７には、各携帯電話機５０毎に、携帯電話機５０のユーザによって設定されたセキュリティレベルが登録されるようにして、中継装置６０では、プログラムの転送先となる携帯電話機５０のセキュリティレベルを特定し、このセキュリティレベルに対応するセキュリティ管理テーブル５０７ａを用いてプログラムの中継可否を判定するようにしてもよい。

【００６６】

（５）第１実施形態において、携帯電話機５０の不揮発性メモリ５０７には、さらに、検査結果表２０２が付与されていないプログラムについて、その実行可否を判定するために用いるセキュリティ管理テーブルが記憶されていてもよい。また、検査機関２０と同様の検査機関が複数ある場合に、検査機関２０とは別の検査機関によって生成された検査結果データが付与されているプログラムについて、その実行可否を判定するために用いるセキュリティ管理テーブルが不揮発性メモリ５０７に記憶されていてもよい。これは、第２実施形態における中継装置６０についても同様であって、ＨＤ６０７には、検査結果表２０２が付与されていないプログラムや、検査機関２０とは別の検査機関によって生成された検査結果データが付与されているプログラムについて、その中継可否を判定するために用いるセキュリティ管理テーブルが記憶されていてもよい。

【００６７】

（６）第１実施形態において、検査結果データ２０２には、コンテンツプロバイダの名称やプログラムの送信元を示すＵＲＬ等、プログラムの提供元を識別するための提供者識別情報をさらに記録するようにして、携帯電話機５０の不揮発性メモリ５０７には、提供者識別情報毎に異なるセキュリティ管理テーブル５０７ａを記憶しておき、携帯電話機５０は、受信した検査結果データ２０２に記録されている提供者識別情報に対応するセキュリ

ティ管理テーブル５０７ａを用いて、受信したプログラムの実行可否を判定するようにしてもよい。第２実施形態についても同様であって、検査結果データ２０２には、提供者識別情報をさらに記録するようにして、中継装置６０のＨＤ６０７には、提供者識別情報毎に異なるセキュリティ管理テーブル５０７ａを記憶しておき、中継装置６０は、受信した検査結果データ２０２に記録されている提供者識別情報に対応するセキュリティ管理テーブル５０７ａを用いて、プログラムの中継可否を判定するようにしてもよい。

【００６８】

（７）第１実施形態において、携帯電話機５０は、プログラムがダウンロードされたときに、このプログラムの検査結果データ２０２とセキュリティ管理テーブル５０７ａとを比較して、このプログラムがセキュリティポリシー（セキュリティ管理テーブル５０７ａ）を満たすプログラムであるか否かを判定し、その判定結果を液晶画面に表示するようにしてもよい。勿論、判定結果は、音声メッセージとして携帯電話機５０から出力されてもよい。また、携帯電話機５０は、受信したプログラムについてユーザが操作入力部５０５を操作してその安全性を検証するよう指示したときに、指示されたプログラムの検査結果データ２０２とセキュリティ管理テーブル５０７ａとを比較して、このプログラムがセキュリティポリシーを満たすプログラムであるか否かを判定し、その判定結果を出力するようにしてもよい。

【００６９】

このように、ネットワークを介して受信したプログラムについて、実行の可否を判定するのではなく、セキュリティポリシーを満たすプログラムであるか否かを判定し、その判定結果をユーザに報知する構成としてもよい。この場合、ユーザは、報知された判定結果に従って、セキュリティポリシーに違反するプログラムであった場合は、このプログラムを不揮発性メモリ５０７から削除（アンインストール）したり、実行しないようにすることができるから、携帯電話機５０のセキュリティを保つことができる。なお、セキュリティポリシーに違反するプログラムであった場合は、このプログラムに含まれていた、使用することが許可されていない関数の名称や、アクセスすることが許可されていないリソースを示す情報を、判定結果とともにユーザに報知する構成としてもよい。また、セキュリティポリシーに違反するプログラムであった場合は、このプログラムを削除するか否かを問うメッセージを液晶画面に表示し、操作入力部５０５から削除する旨が指示された場合に、このプログラムを不揮発性メモリ５０７からアンインストールする構成としてもよい。

【００７０】

また、第２実施形態において中継装置６０は、携帯電話機５０へプログラムを転送するときに、転送するプログラムの検査結果データ２０２と、セキュリティ管理テーブル５０７ａとを比較して、このプログラムがセキュリティポリシー（セキュリティ管理テーブル５０７ａ）を満たすプログラムであるか否かを判定し、その判定結果をプログラムとともに携帯電話機５０へ送信するようにしてもよい。

【００７１】

（８）第１実施形態における携帯電話機５０を以下のように変形してもよい。

すなわち、携帯電話機５０は、コンテンツサーバ１０ａからプログラムをダウンロードする前に、まず、ダウンロードするプログラムの検査結果データ２０２のみをコンテンツサーバ１０ａから受信する。次いで、携帯電話機５０は、受信した検査結果データ２０２とセキュリティ管理テーブル５０７ａとを比較して、ダウンロードしようとしているプログラムが、セキュリティポリシー（セキュリティ管理テーブル５０７ａ）を満たすプログラムであるか否かを判定する。その結果、携帯電話機５０は、セキュリティポリシーを満たすプログラムであった場合は、このプログラムをコンテンツサーバ１０ａからダウンロードする一方、セキュリティポリシーに違反するプログラムであった場合は、このプログラムのダウンロードを中止する。このような構成とすれば、セキュリティポリシーに違反するプログラムであった場合には、このプログラムのダウンロードを事前に中止することができるから、無駄なパケット通信を行わずに済む。

【００７２】
（９）第１および第２実施形態では、プログラムをダウンロードする場合について説明したが、勿論、プログラムを携帯電話機５０に配信する場合についても本発明を適用することができる。また、本発明に係る受信装置を、公衆無線ＬＡＮを介して通信を行う無線端末や、インターネットを介して通信を行うパーソナルコンピュータ等に適用してもよい。また、本発明に係る中継装置を、ゲートウェイサーバやプロキシサーバ、移動パケット通信網４０に設けられた交換局や基地局等に適用してもよい。また、本発明に係る処理を携帯電話機５０や中継装置６０等のコンピュータに実行させるためのプログラムは、通信によってコンピュータにインストールされてもよい。また、コンピュータによって読み取り可能な各種の記録媒体に上記プログラムを記録して頒布してもよい。

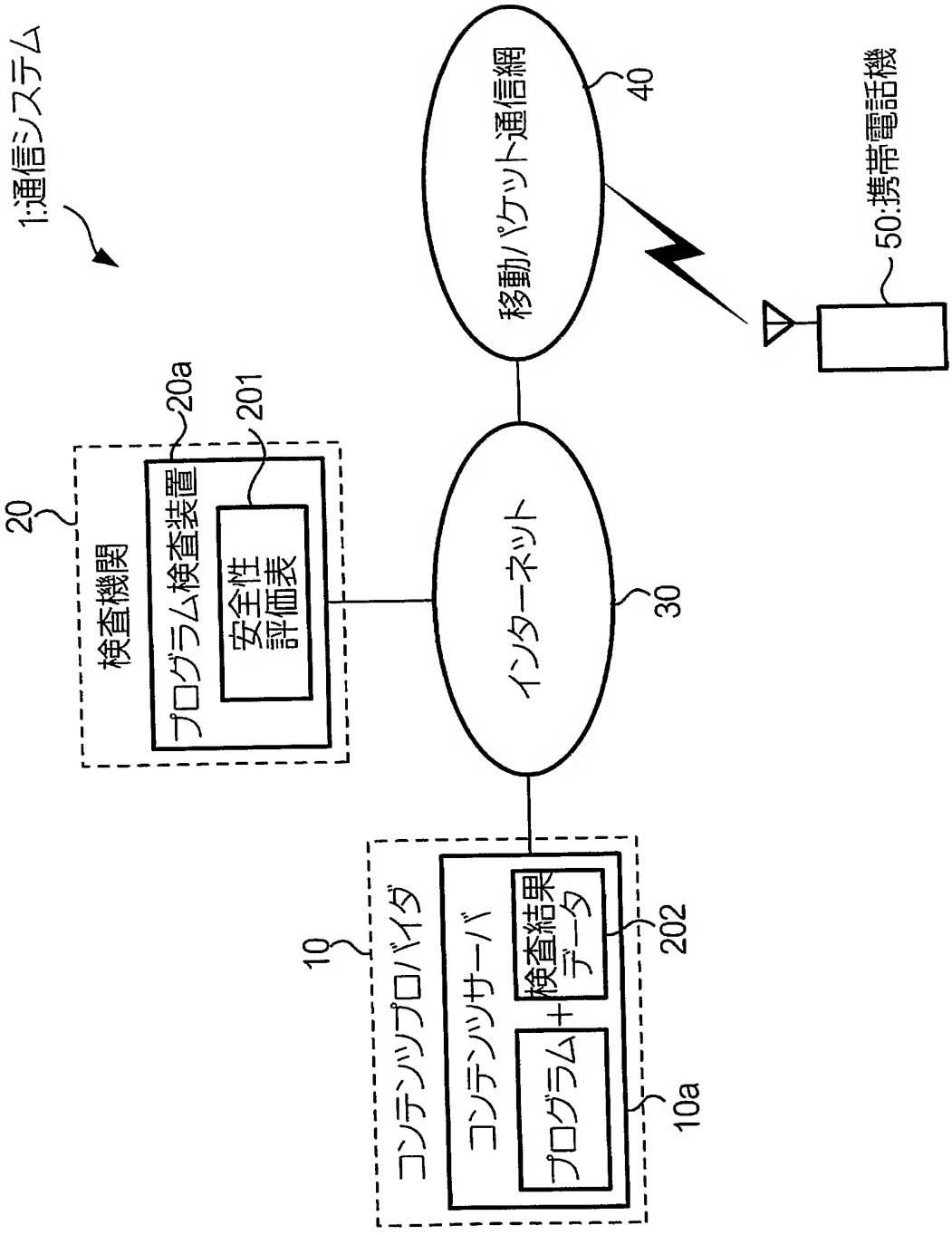
【図面の簡単な説明】

【００７３】
【図１】第１実施形態に係る通信システム１の構成を例示するブロック図である。
【図２】同実施形態に係り、検査結果データ２０２のデータ構成を例示する図である。
【図３】同実施形態に係り、携帯電話機５０のハードウェア構成を例示するブロック図である。
【図４】同実施形態に係り、セキュリティ管理テーブル５０７ａのデータ構成を例示する図である。
【図５】同実施形態に係り、プログラムとその検査結果データ２０２が携帯電話機５０にダウンロードされるまでの通信システム１各部の動作について例示するシーケンスチャートである。
【図６】同実施形態に係り、セキュリティレベルを設定する際の携帯電話機５０の画面表示例を示す図である。
【図７】同実施形態に係り、携帯電話機５０において実行される、ネットワークを介して受信したプログラムの実行可否を判定する処理の動作を例示するフローチャートである。
【図８】同実施形態に係り、プログラムの実行が許可されなかった場合の携帯電話機５０の画面表示例を示す図である。
【図９】第２実施形態に係り、中継装置６０のハードウェア構成を例示するブロック図である。
【図１０】同実施形態に係り、中継装置６０において実行される、プログラムの中継可否を判定する処理の動作を例示するフローチャートである。
【図１１】変形例（１）に係る通信システム２の構成を例示するブロック図である。
【図１２】変形例（２）に係る携帯電話機５０において実行される処理の動作を例示するフローチャートである。
【図１３】変形例（２）に係る携帯電話機５０の画面表示例を示す図である。

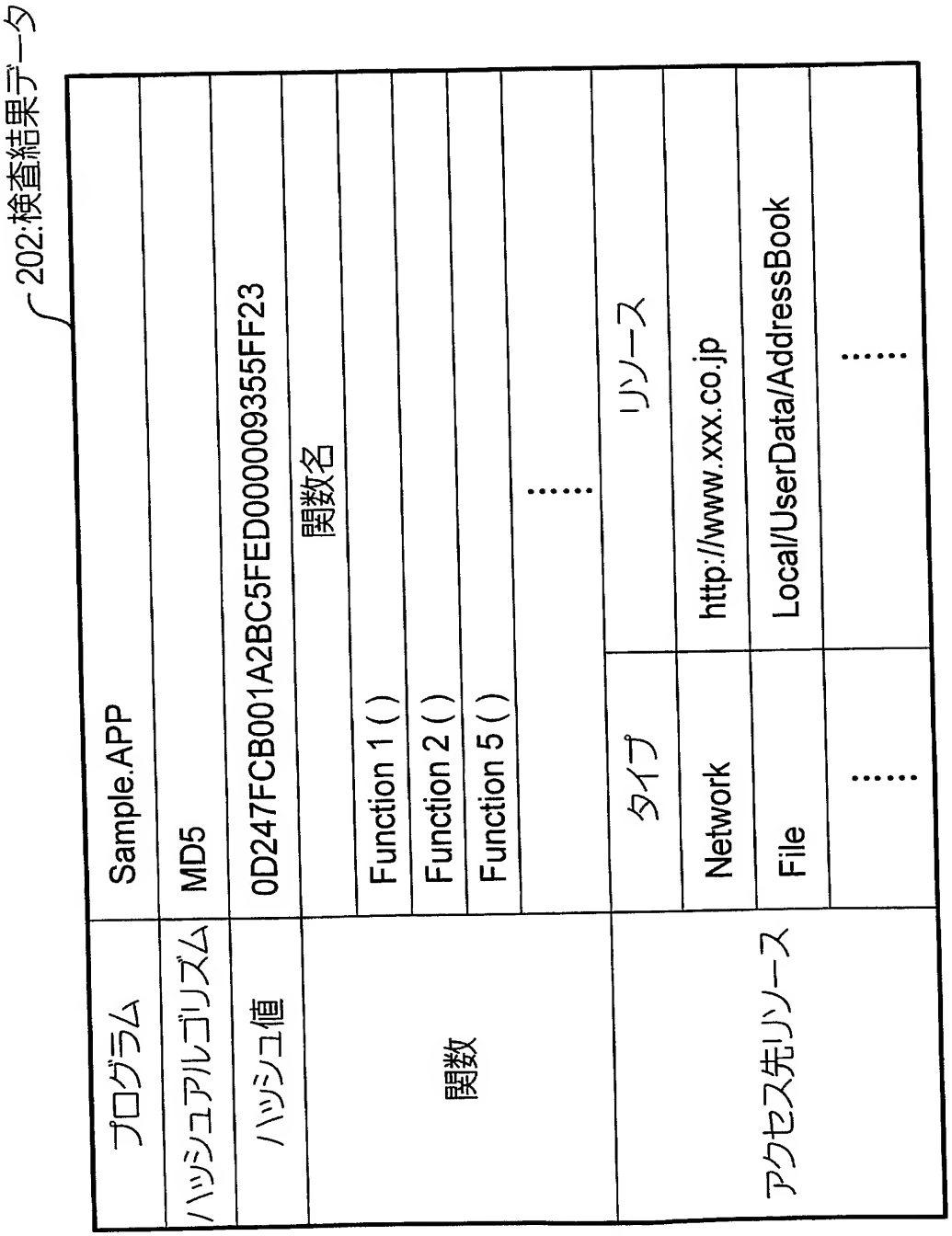
【符号の説明】

【００７４】
１，２…通信システム、１０…コンテンツプロバイダ、１０ａ，１０ｂ…コンテンツサーバ、２０…検査機関、２０ａ…プログラム検査装置、３０…インターネット、４０…移動パケット通信網、５０…携帯電話機、６０…中継装置、７０…検査結果登録サーバ、２０１…安全性評価表、２０２…検査結果データ、５０１…ＣＰＵ、５０２…ＲＯＭ、５０３…ＲＡＭ、５０４…無線通信部、５０５…操作入力部、５０６…液晶表示部、５０７…不揮発性メモリ、５０７ａ…セキュリティ管理テーブル、６０１…ＣＰＵ、６０２…ＲＯＭ、６０３…ＲＡＭ、６０４…通信インタフェース、６０５…操作入力部、６０６…表示部、６０７…ＨＤ。

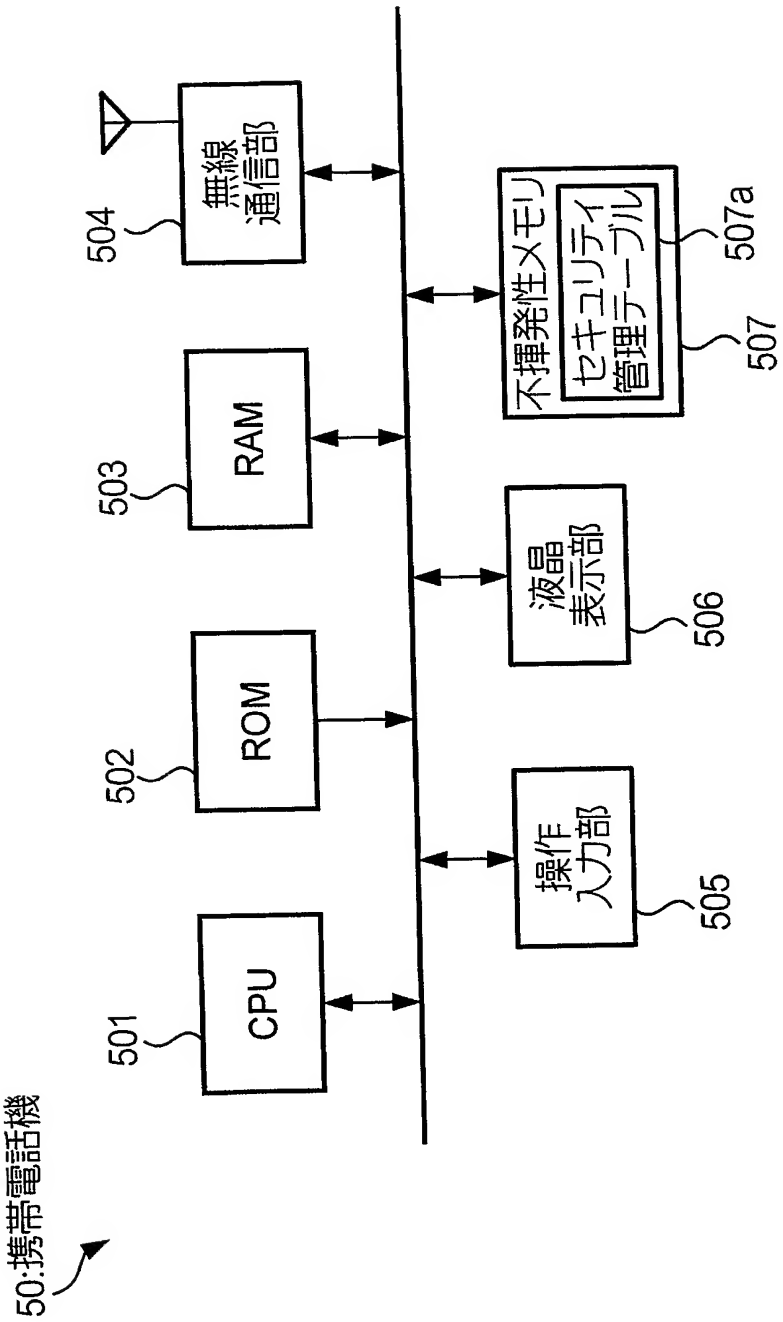
【書類名】図面
【図１】


1:通信システム
移動パケット通信網
40
50:携帯電話機
20a
201
20
検査機関
プログラム検査装置
安全性評価表
インターネット
30
10
コンテンツプロバイダ
コンテンツサーバ
プログラム
検査結果データ
202
10a

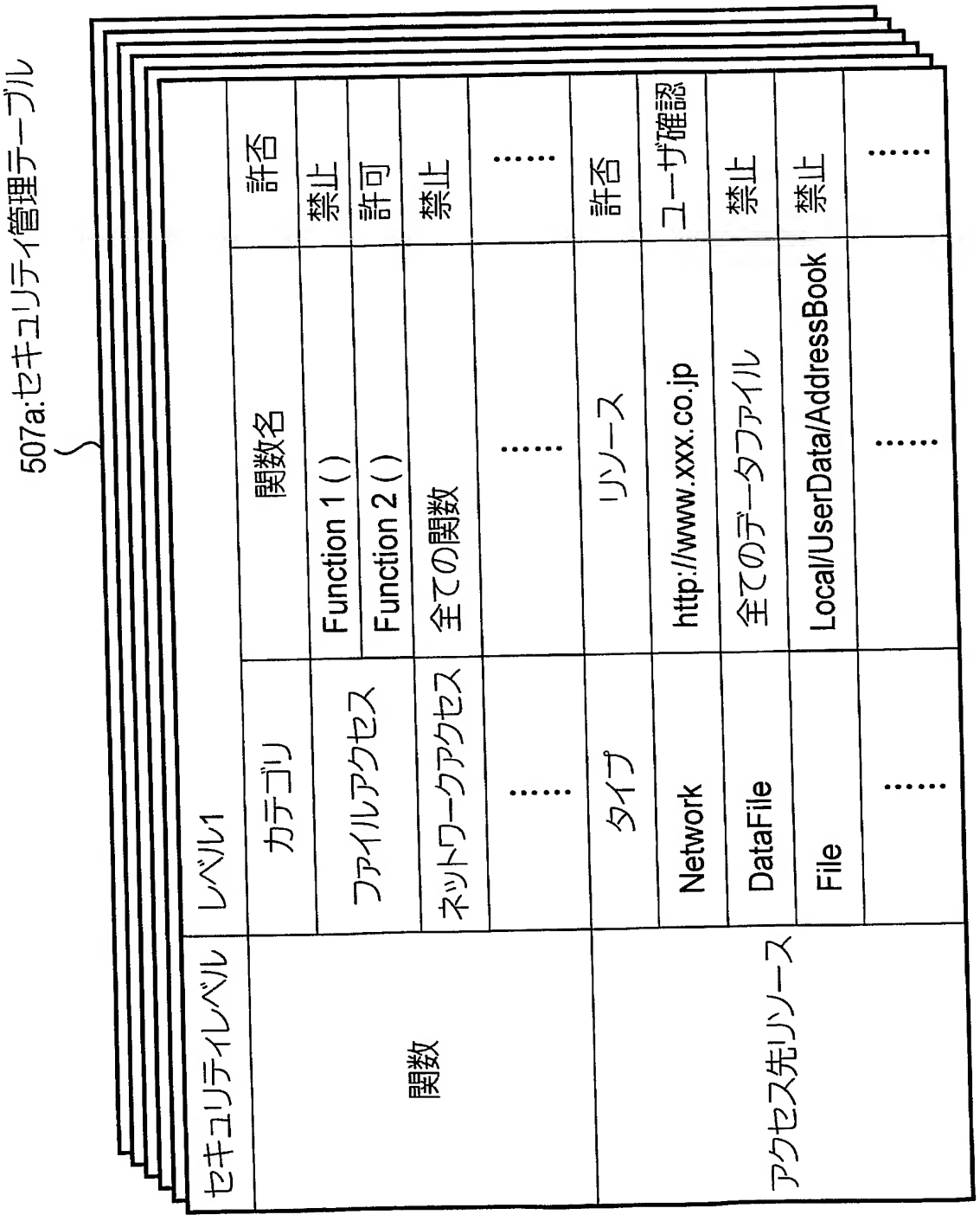
【図２】


202:検査結果データ
プログラム
Sample.APP
ハッシュアルゴリズム
MD5
ハッシュ値
0D247FCB001A2BC5FED0000009355FF23
関数
関数名
Function 1 ( )
Function 2 ( )
Function 5 ( )
アクセス先リソース
タイプ
リソース
Network
http://www.xxx.co.jp
File
Local/UserData/AddressBook

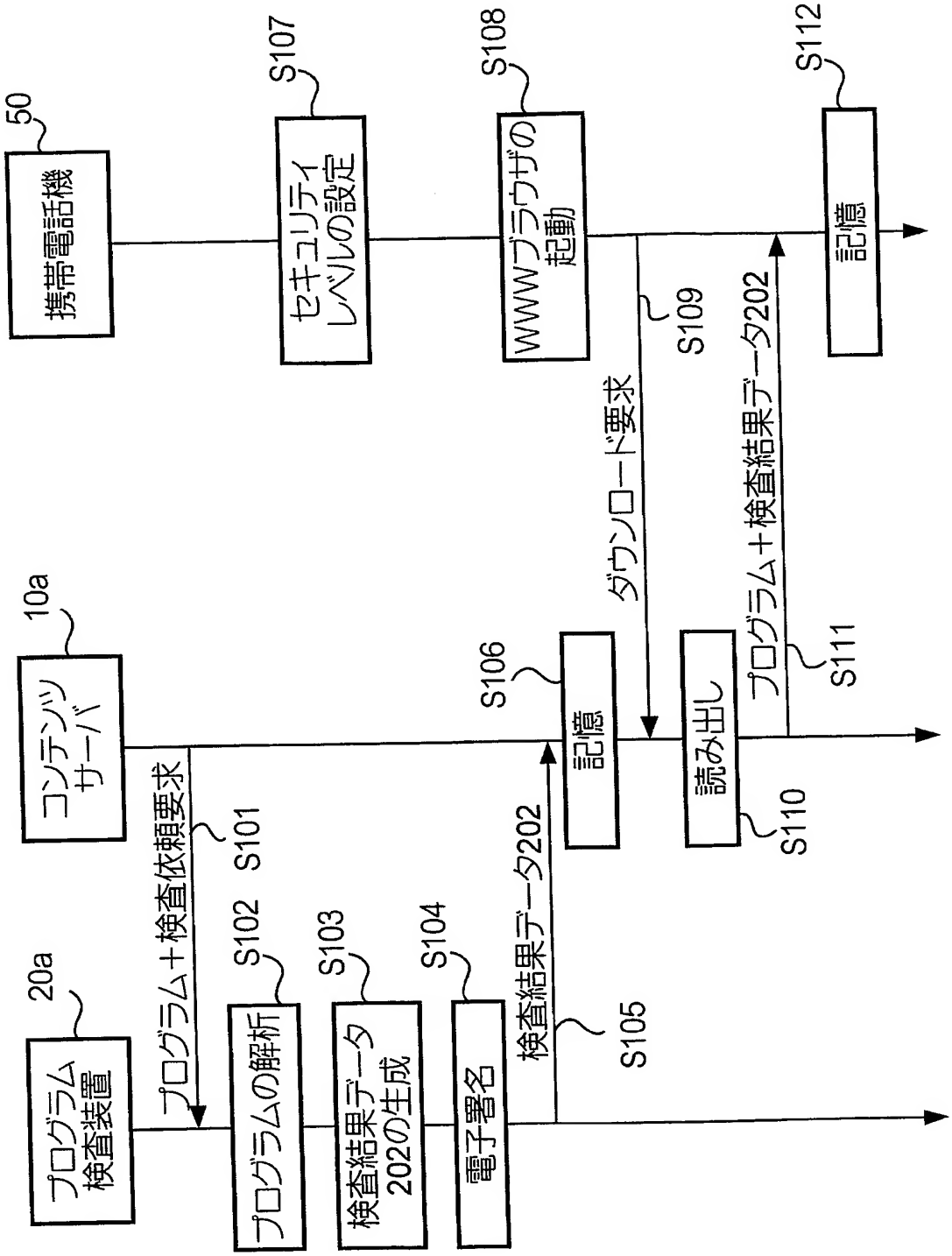
【図３】


50:携帯電話機
501
CPU
502
ROM
503
RAM
504
無線
通信部
505
操作
入力部
506
液晶
表示部
507
不揮発性メモリ
セキュリティ
管理テーブル
507a

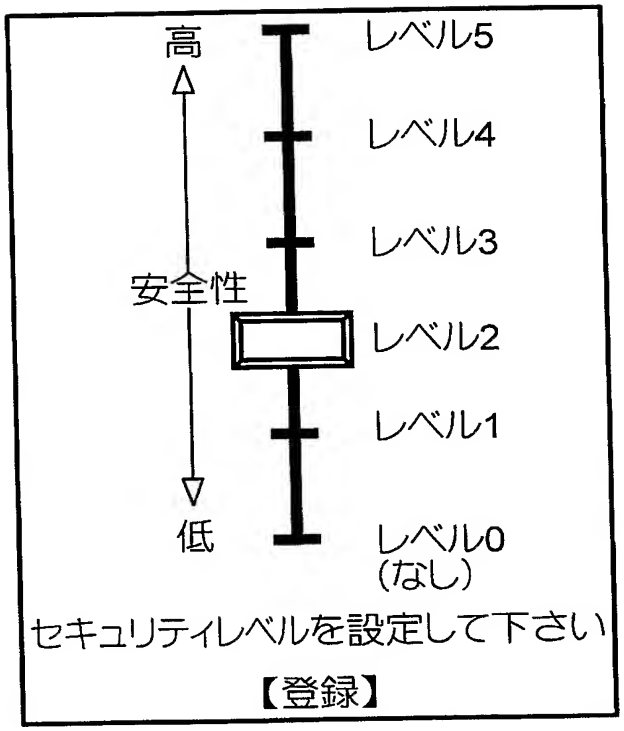
【図４】


507a:セキュリティ管理テーブル
セキュリティレベル
レベル1
関数
カテゴリ
関数名
許否
ファイルアクセス
Function 1 ( )
禁止
Function 2 ( )
許可
ネットワークアクセス
全ての関数
禁止
……
……
……
アクセス先リソース
タイプ
リソース
許否
Network
http://www.xxx.co.jp
ユーザ確認
DataFile
全てのデータファイル
禁止
File
Local/UserData/AddressBook
禁止
……
……
……

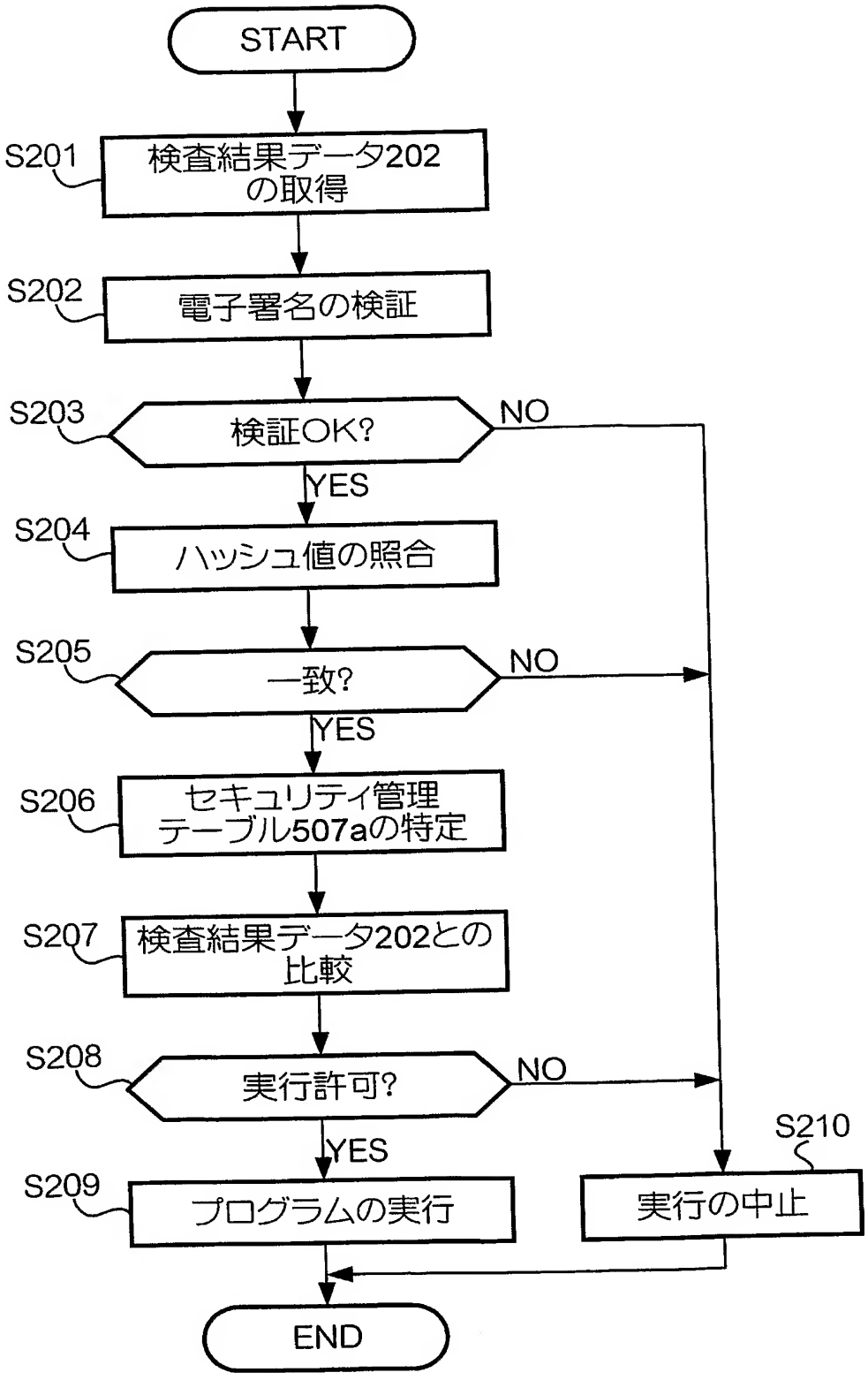
【図５】


50
携帯電話機
S107
セキュリティレベルの設定
S108
WWWブラウザの起動
S112
記憶
S109
ダウンロード要求
プログラム＋検査結果データ202
S111
10a
コンテンツサーバ
S106
記憶
読み出し
S110
プログラム＋検査依頼要求
S101
20a
プログラム検査装置
S102
プログラムの解析
S103
検査結果データ202の生成
S104
電子署名
検査結果データ202
S105

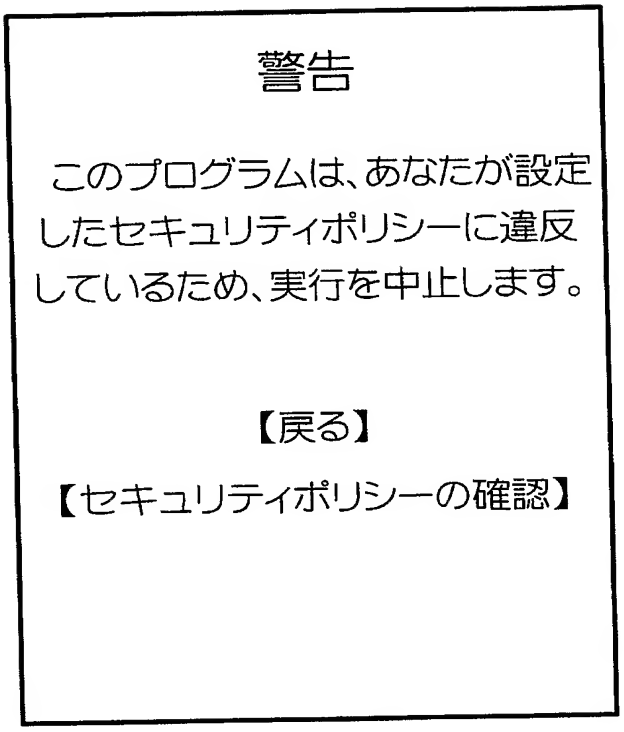
【図６】


高
安全性
低
レベル5
レベル4
レベル3
レベル2
レベル1
レベル0
(なし)
セキュリティレベルを設定して下さい
【登録】

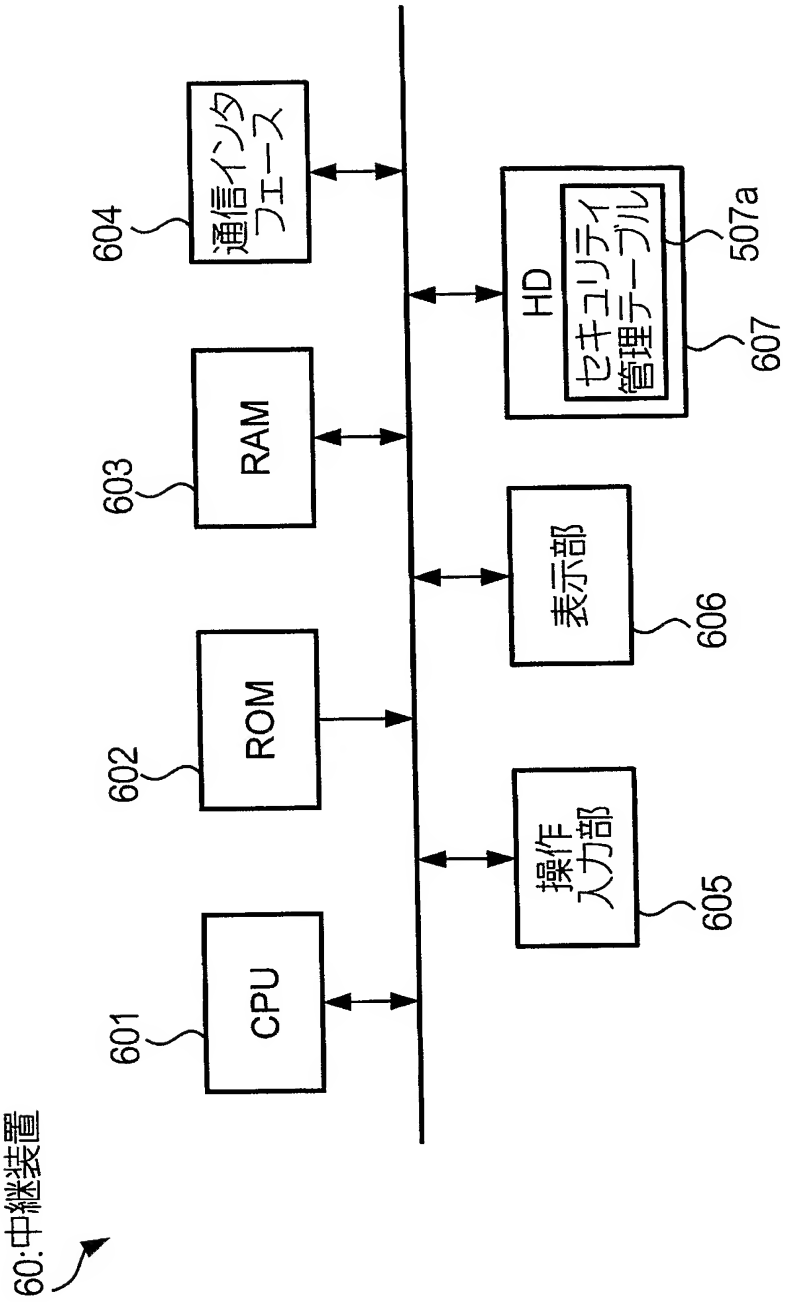
【図７】


START
S201
検査結果データ202の取得
S202
電子署名の検証
S203
検証OK?
NO
YES
S204
ハッシュ値の照合
S205
一致?
NO
YES
S206
セキュリティ管理テーブル507aの特定
S207
検査結果データ202との比較
S208
実行許可?
NO
YES
S209
プログラムの実行
S210
実行の中止
END

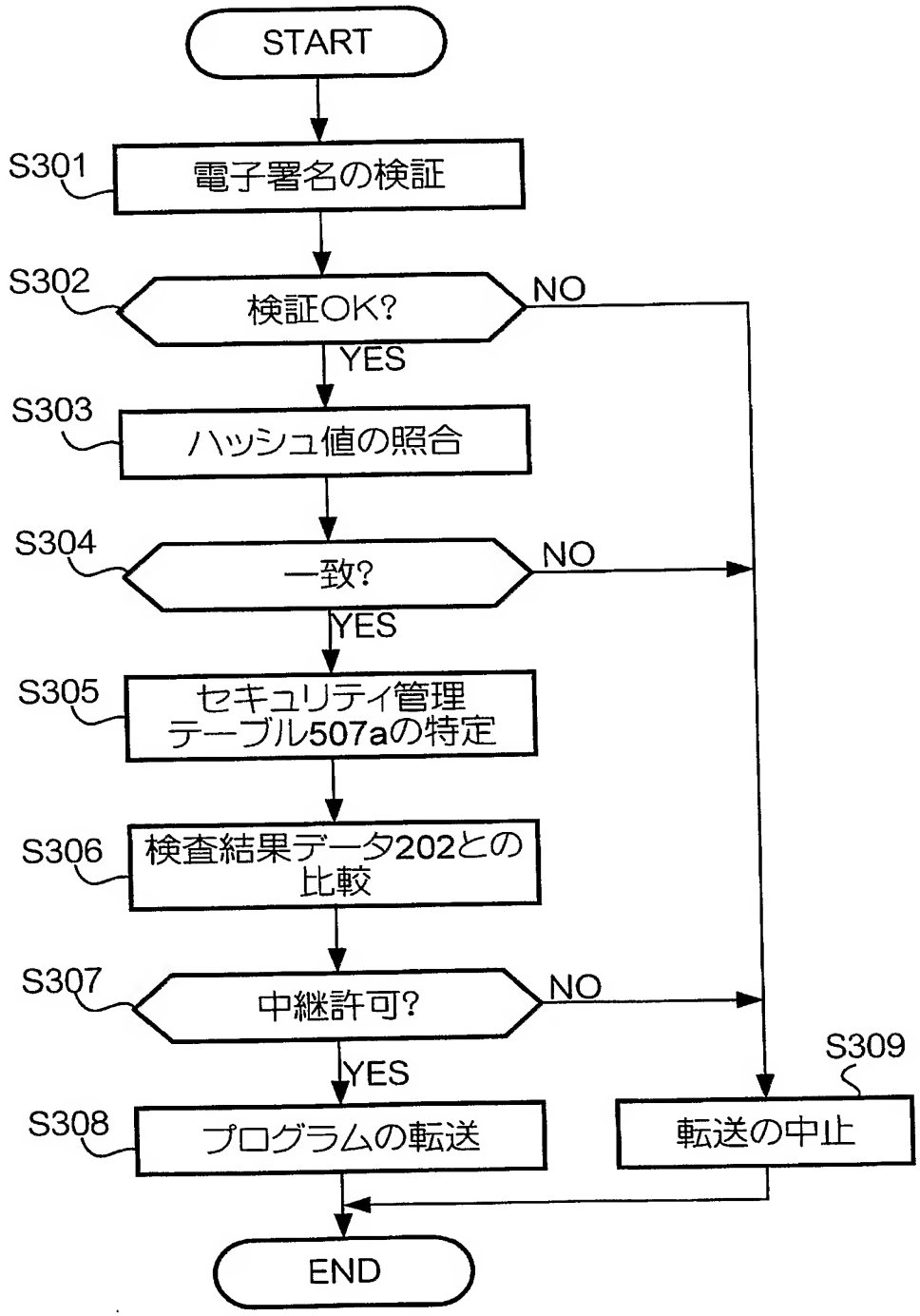
【図８】


警告
このプログラムは、あなたが設定したセキュリティポリシーに違反しているため、実行を中止します。
【戻る】
【セキュリティポリシーの確認】

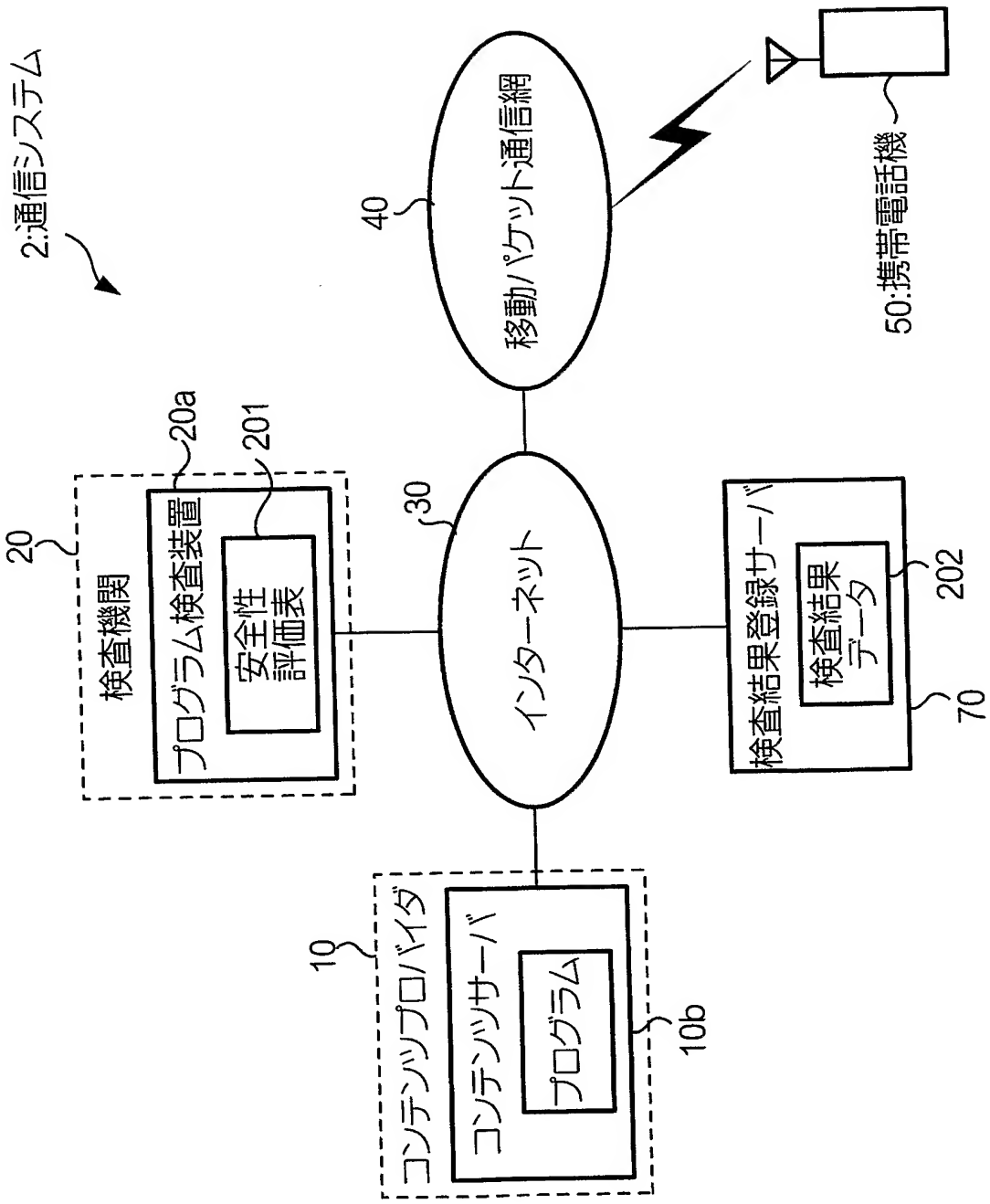
【図９】


60:中継装置
601
CPU
602
ROM
603
RAM
604
通信インタフェース
605
操作入力部
606
表示部
607
HD
セキュリティ管理テーブル
507a

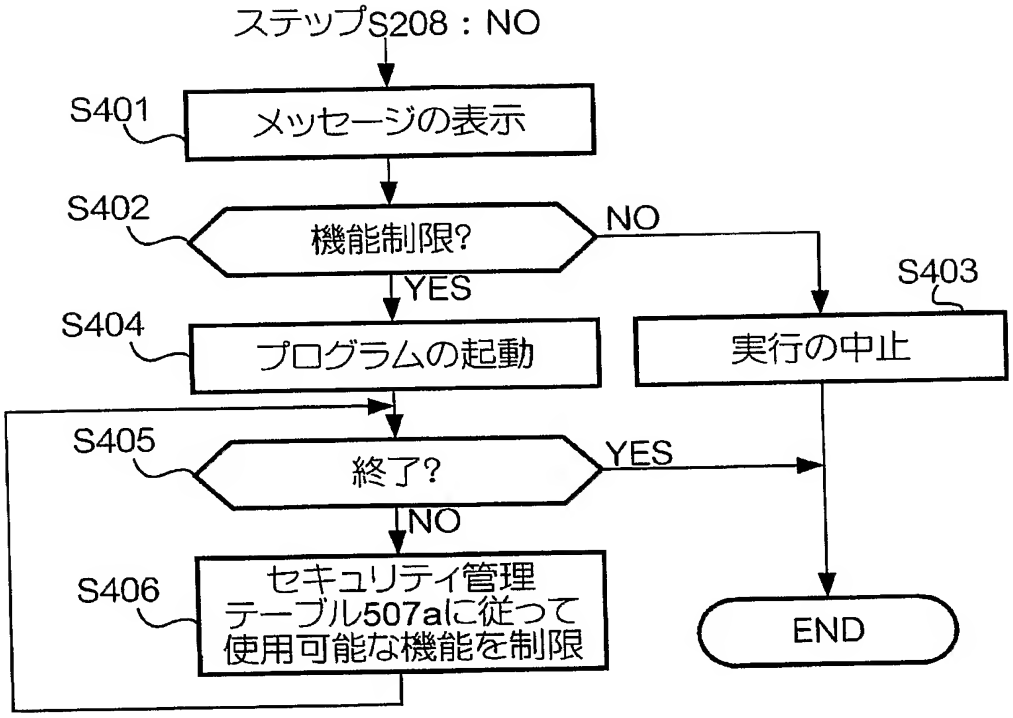
【図１０】


START
S301
電子署名の検証
S302
検証OK?
NO
YES
S303
ハッシュ値の照合
S304
一致?
NO
YES
S305
セキュリティ管理
テーブル507aの特定
S306
検査結果データ202との
比較
S307
中継許可?
NO
YES
S308
プログラムの転送
S309
転送の中止
END

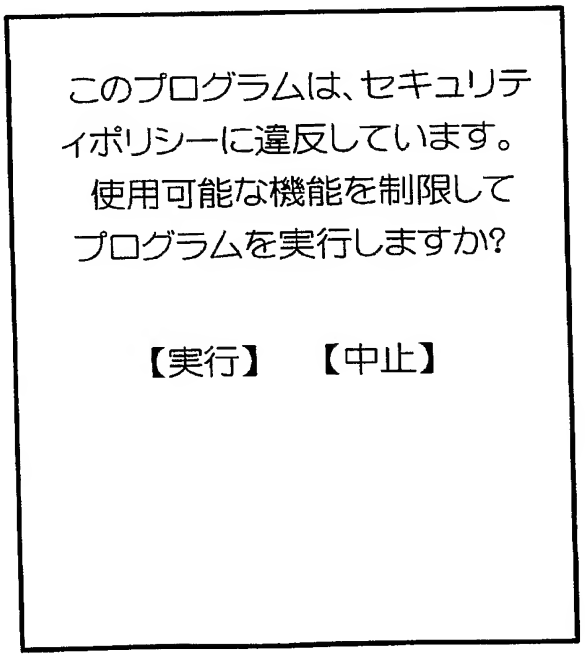
【図１１】


2:通信システム
40
移動パケット通信網
50:携帯電話機
20a
201
20
検査機関
プログラム検査装置
安全性評価表
30
インターネット
検査結果登録サーバ
検査結果データ
202
70
10
コンテンツプロバイダ
コンテンツサーバ
プログラム
10b

【図１２】


ステップS208：NO
S401
メッセージの表示
S402
機能制限?
NO
YES
S403
実行の中止
S404
プログラムの起動
S405
終了?
YES
NO
S406
セキュリティ管理
テーブル507aに従って
使用可能な機能を制限
END

【図１３】


このプログラムは、セキュリティポリシーに違反しています。
使用可能な機能を制限してプログラムを実行しますか?
【実行】
【中止】

【書類名】要約書
【要約】
【課題】　ネットワークを介して提供されるプログラムがセキュリティ上、問題のあるプログラムであるか否かを、受信装置や中継装置において簡易な構成で短時間のうちに判定できるようにすること。
【解決手段】　プログラム検査装置２０ａは、ネットワークを介して携帯電話機５０に提供されるプログラムの内容を事前に検査し、このプログラムに含まれている関数や、このプログラムを実行した場合にアクセスされるリソースを示す情報を記録した検査結果データ２０２を生成する。携帯電話機５０は、各関数についての使用許否や、各リソースについてのアクセスの許否が登録されたセキュリティ管理テーブル５０７ａを有しており、ネットワークを介して受信したプログラムについて、このプログラムの検査結果データ２０２と、セキュリティ管理テーブル５０７ａとを比較して、このプログラムを実行した場合にセキュリティ上の問題が起きないか判定する。
【選択図】　図１

【書類名】　手続補正書
【提出日】　平成16年12月 2日
【あて先】　特許庁長官　殿
【事件の表示】
　【出願番号】　特願2004- 29928
【補正をする者】
　【識別番号】　397011166
　【氏名又は名称】　トレンドマイクロ株式会社
【代理人】
　【識別番号】　100098084
　【弁理士】
　【氏名又は名称】　川▲崎▼　研二
　【電話番号】　03-3242-5481
【手続補正1】
　【補正対象書類名】　特許願
　【補正対象項目名】　発明者
　【補正方法】　変更
　【補正の内容】
　　【発明者】
　　【住所又は居所】　東京都渋谷区代々木２－１－１　トレンドマイクロ株式会社内
　　【氏名】　近藤　賢志
　　【発明者】
　　【住所又は居所】　東京都渋谷区代々木２－１－１　トレンドマイクロ株式会社内
　　【氏名】　谷田部　茂
【その他】　平成１６年２月５日付出願の特願２００４－２９９２８号の特許願の発明者の氏名を「近藤　賢志」「谷田部　茂」と記するところを誤って「近藤　賢志」「矢田部　茂」として出願してしまいました。上記氏名の誤記を訂正いたしたく本書を提出致しますので、宜しくお願い申し上げます。

特願２００４－０２９９２８

出　願　人　履　歴　情　報

識別番号　［３９７０１１１６６］

１．変更年月日　２００３年１１月２６日
［変更理由］　住所変更
住　所　東京都渋谷区代々木２－１－１　新宿マインズタワー
氏　名　トレンドマイクロ株式会社